EXHIBIT A

MAZIE SLATER KATZ & FREEMAN, LLC
COUNSELLORS AT LAW
103 Eisenhower Parkway
Roseland, NJ 07068
(973) 228-9898
Fax (973) 228-0303
www.mazieslater.com

David A. Mazie*
Adam M. Slater*°
Eric D. Katz*°
David M. Freeman
Beth G. Baldinger
Matthew R. Mendelsohn°

Karen G. Kelsen°
Cheryll A. Calderon
David M. Estes
Adam M. Epstein°
Michael R. Griffith°
Matthew Tonzola
Christopher J. Geddis

*Certified by the Supreme Court of New Jersey as a Civil Trial Attorney

°Member of N.J. & N.Y. Bars

April 8, 2019

VIA EMAIL
SAGoldberg@duanemorris.com
Seth A. Goldberg, Esq.
Duane Morris LLP
30 South 17th Street
Philadelphia, Pennsylvania 19103-4196

Dear Mr. Goldberg:

Per our discussion this morning, attached is the Plaintiffs' proposed ESI protocol, which is based on the Benicar ESI Protocol, and utilizes most of the language used in Benicar.

In addition, as also discussed, in order to most efficiently move forward with the collection and production of documents in this matter, and pursuant to the Court's stated desire that such matters be resolved in a cooperative manner to the extent feasible, Plaintiffs request the following information concerning Defendants' documents and ESI to aid the Plaintiffs in finalizing the ESI protocol and constructing our document storage system. We are hopeful that the Defendants will each agree to provide the requested information without the need to involve the Court. We are prepared to meet and confer on any ESI issues you see in this letter or the attached Protocol.

A. Document Retention Policies

1. Produce all document retention and/or records management policies and procedures for all defendants, and for each provide documentation and/or on Affidavit with supporting documentation setting forth:

   a. Author(s) of the policy or procedure.

b. Custodian(s) of the policy or procedure.
c. When the policy was implemented, and dates (MM/DD/YYYY) of first and last use.
d. Dates of all revisions, along with all drafts and revisions.
e. Department responsible for the enforcement and implementation of the policies and procedures.

2. Produce all litigation hold letters and notices applicable to the Valsartan products at issue, draft and final, for all defendants, and all documentation of compliance or non-compliance therewith.

3. Confirm whether any documents that are relevant to any of the issues in this litigation have been destroyed, discarded, or are otherwise no longer available, and documentation of efforts to make this determination.

4. Produce all CAPAs (Corrective Action Prevention Action) with regard to document, information, or data management or preservation, and full documentation of the handling or resolution thereof.

5. Produce all policies related to the preservation of the desktops/laptops/mobile devices/data/documents/information of former employees and the data therein.

B. Internal Company Files

1. Produce a list of all potential sources and locations of paper documents that are relevant to the issues in this litigation.

2. Provide the earliest date on which documents related to the drugs at issue exists in each defendant's files.

3. Produce a list of all file types and extensions that actually appear and/or exist in the names of or within files that contain relevant documents, including but not limited to relevant emails or other communications, and identify the software used to create and/or access such files.

C. Technology Assisted Review ("TAR") and Search Terms

1. Confirm whether defendants have used or intend to use TAR (including predictive coding) for searching, locating, determining the relevancy of, or review of documents, and, if so, provide documentation describing:

    a. The manner in which TAR has been or will be applied and used
    b. The selection of underlying data on which the TAR will be applied and used
    c. The identity of the vendor being utilized
    d. The identity of the TAR software being utilized.
    e. Precision
    f. Recall goals
    g. Validation methods
    h. Any further review or culling of the results of the TAR for relevancy
    i. All "seed sets" or test sets of documents, terminology, or other documents or information utilized in conjunction with TAR

2. Confirm whether defendants have used or are intend to use search terms for searching, locating, determining the relevancy of, or review of documents, and, if so, provide documentation describing:

    a. The manner in which search terms have been or will be applied and used
    b. The selection of underlying data on which the search terms will be applied and used
    c. The search terms and any modifiers that have been or will be applied and used
    d. The identity of the vendor being utilized
    e. The identity of the search software being utilized
    f. Validation methods
    g. Any further review or culling of the results from the application of search terms for relevancy

3. Confirm whether defendants have used or intend to use TAR and/or search terms for searching, locating, determining the relevancy of, or review of

foreign language documents and, if so, provide the same information asked for above in C.1 and C.2 as to each language.

D. Network Servers

1. Provide a description of any network based system and topology utilized by defendants and provide documentation describing:

   a. The number and types of computers/servers utilized and their locations.
   b. All operating systems installed on any computers/servers.
   c. All software applications used at any time during the relevant time frame.

2. Describe all intranets, communications systems, file storage systems, document management systems, and database systems accessible to any employees that may contain, or have contained, potentially relevant information during the entire relevant time period.

3. Confirm whether the company maintains servers at any of the company's divisions/business units/locations/offices/subsidiaries/affiliates/vendors that exist separately from or in addition to company-wide server(s), and if so, describe to what extent any of those servers may store any potentially relevant information.

4. Produce any index, network topology, or ESI Data map that exists of defendants' IT systems.

5. Describe the backup system of each of defendants' computers, servers, workstations, and devices (by category) and provide documentation describing the following:

   a. Hardware and software used to back up and archive information.
   b. Identification of what data is backed up.
   c. The dates for which backup data is available.
   d. Backup schedules.
   e. Locations of all backup media devices.

f. Identification of any of any third party backup/storage/archiving product or location utilized by defendants.

g. The format of the backup, including but not limited to the type of media on which such backups are stored, and the location of such media.

E. Email/Messaging/Communications Servers/Systems

1. Identify the systems used for any exchange of communications by your employees, including but not limited to email, instant messaging, text messaging, imessaging, SMS, MMS, chat rooms, list-servers, discussion forums, voicemail, voice-chat, video-chat, video-conferencing, and shared data stores, and the time period for the use of each system, including any systems used at any overseas facilities; and provide documentation describing the following:

   a. Server, workstation, and device software and version.
   b. List of users utilizing the systems.
   c. Location of communication files.
   d. All software and/or applications used on such systems.
   e. Names and locations of servers, workstations, and devices.

2. Identify communications servers at any or all of the company's divisions/business units/locations/offices/subsidiaries that exist separately or in addition to the company-wide server(s).

3. Indicate whether any end-user communications are stored on (i) the end-user's hard drive, (ii) servers, (iii) a server of a third party application service provider, or (iv) a mobile device.

4. If any of defendants' communications systems have changed during the relevant time period, identify any legacy system(s), the current system(s), the date range for which information is available on each system, and the date(s) of the backup(s) made with each relevant legacy system.

5. Describe the backup system of each of defendants' communications servers and devices and provide documentation describing the following:

   a. Hardware and software used to back up and archive information.

b. Identification of what data and information is backed up.
c. The dates for which backup data is available.
d. Backup schedules.
e. Locations of all backup media devices.
f. Identification of any third party backup/storage/archiving product utilized by defendants.
g. The format of the backup, including but not limited to the type of media on which such backups are stored, and the location of such media.

6. Produce all company policies related to how employees access their email and other communications on mobile devices or personal devices and provide a description of how the data from the mobile device and email or other communications client are synced.

F. Hard Drives/Devices

1. Produce all company policies governing the backup of employees' desktop and laptop hard drives and other devices, including but not limited to cellphones, smartphones, tablets, USB drives, and PDAs.

2. Describe defendants' efforts to determine the extent to which any of the key custodians in this litigation have relevant information which is located on such hard drives and other devices..

3. Confirm whether at any time such hard drives and other devices were or are erased, "wiped," "scrubbed," or reformatted.

4. Produce all company policies related to "approved" communication applications, including but not limited to text messaging/instant messaging applications or other third party applications such as Salesforce.com.

G. Non-Company Computers/Devices

1. Produce all company policies governing employee use of computers or other devices not owned or controlled by the company to create, receive, store, or send work-related documents or communications.

2. Identify all third-party systems and applications, including but not limited to cloud-based systems and applications, that may contain relevant data, and all policies and procedures that are relevant thereto.

3. Produce all documentation relating to any BYOD ("Bring Your Own Device") policy in place.

H. Key Custodians of Potentially Relevant Information

1. Identify the key custodians of potentially relevant information and provide documentation describing:
   a. Name
   b. Company by which custodian was employed
   c. Department(s)
   d. Title(s)
   e. Job description(s)
   f. Dates of employment, and at each position
   g. Sources of custodial information (i.e., e-mail, paper files, laptop, ipad)
   h. Size of custodial file (if known)
   i. All non-custodial sources to which the custodian had access
   j. All non-custodial sources for which the custodian had responsibility
   k. All test results for searches of custodian to date (if conducted)

2. Identify custodian(s) responsible for maintaining/administering each of the company's electronic information systems.

3. Identify any third parties that may hold potentially relevant information and provide documentation describing to what extent information in the possession, custody, or control of third parties has been preserved. This includes but is not limited to marketing drafts of documents, clinical study data and documentation, and research and development laboratory testing and data. Describe what efforts have been undertaken to date and what, if any, additional efforts are underway.

Very truly yours,

ADAM M. SLATER